



Interested in learning more about security?

SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Third-Party Mail Relay (Open Relay) and Microsoft Exchange Server

In the following paper I will be discussing the topic of Third Party Mail Relay, or Open Relay, the SMTP protocol, and the unwanted side affects of having a system that is configured as an open relay. Next I will go over the procedure of configuring Microsoft's email server software, called Exchange, so that it is not an open relay.

Copyright SANS Institute
Author Retains Full Rights

AD

A banner advertisement for FireEye. On the left is the FireEye logo, which consists of a stylized red and white flame/eye shape next to the word "FireEye" in a sans-serif font. To the right of the logo is a black background with white and red text. The text reads: "Protect critical data from the cyber theft pandemic." followed by "Learn how in this FireEye white paper." On the far right of the banner is a small image of a man in a hard hat looking at a computer screen that displays a yellow bird in a cage.

Protect critical data from the cyber theft pandemic.
Learn how in this FireEye **white paper.**

Third Party Mail Relay (Open Relay) and Microsoft Exchange Server

Introduction

In the following paper I will be discussing the topic of Third Party Mail Relay, or Open Relay, the SMTP protocol, and the unwanted side affects of having a system that is configured as an open relay. Next I will go over the procedure of configuring Microsoft's email server software, called Exchange, so that it is not an open relay.

What is third party mail relay or open relay?

It is the ability of an email server to receive email from an unknown sender and then sending it on to a recipient or recipients, which could number in the thousands, that are not users of that email system.

The protocol responsible for relaying is called SMTP or Simple Mail Transfer Protocol. This protocol belongs to the TCP/IP family and is used by email servers to transfer email from the senders email server to the recipient or recipients' email server or servers. The default port that it works on is port 25.

The sole responsibility of SMTP is to relay email from the host to the recipient's email server. It is the responsibility of the email administrator to restrict this relaying function so that it is not an open relay, but a controlled relay. This is done in different ways depending on the email server platform. With some older versions of email servers, Exchange being one of them, you do not have any way to restrict the SMTP relay functionality. To get a detailed explanation of the SMTP protocol and how it works see the Internet Engineering Task Force's (IETF) Request for Comments (RFC) 821 and 822 located at www.ietf.org.

It is also possible for you to telnet directly to an SMTP server by starting a telnet session by typing the following command:

```
telnet [server name] [port number]
```

The server will reply with a 220 message indicating that it is ready. Other commands that you can use are *HELO*, *MAIL FROM:*, and *RCPT TO*.

The consequences of running your email server as an open relay can be great. The greatest threat comes in the form of Unsolicited Commercial Email (UCE) or SPAM. Besides being very annoying SPAM has been and is becoming a very big problem, with some very serious side effects, for the Internet community. It has become such a problem that the IETF released RFC 2505 "Anti-Spam Recommendations for SMTP MTAs" in February of 1999 to address this threat.

Depending on the amount of UCE being sent through the email system, it could cause a Denial of Service (DoS) situation where the server is unable to process legitimate email or bring your network to a crawl. This network congestion results in wasted resources and wasted time and thus wasted money for your organization. Also if the server is unable to handle the mass amount of UCE it could cause it to crash by filling up hard drives with large email queues and log files.

Having your server configured as an open relay long enough is a sure way to get it into anti-SPAM organizations databases of open relays called Blacklists. These databases are used by many organizations to block UCE from getting into their email systems. Two well-known organizations are Open Relay Behaviour-modification System (ORBS) and Mail Abuse Prevention System (MAPS). More information about these two organizations can be found at www.orbs.org and www.mail-abuse.org respectively. This can start to cause you as the email administrator some serious problems with your users as they will be unable to send their email to any of the domains that has your server on their blacklist.

Another serious risk of having your email server configured as an open relay is the ability of a hacker to pose as an internal user by sending email to other users on your network requesting vital network information such as logon names, passwords, etc.

If the above threats are not enough to get your attention then your company's management will when it gets wind that their company is associated with large volumes of UCE and is suffering from a public perception problem because of it.

One last problem that can cause you headaches with an open relay system is that of a legal issue. For a good legal reference on UCE in the United States (Federal and State), European Union, as well as many other countries check out www.spamlaws.com.

Exchange Server

In this section I will detail the process of configuring Microsoft's Exchange Server as to preventing it from being an open relay server.

Exchange Versions

With versions of Exchange Server below 5.0 it is impossible to configure the server to be a secured relay. If your Exchange Server version is below version 5.0 the recommended path is to upgrade to at least Exchange server 5.5 Service Pack 2 with the encapsulated SMTP relay address patch. If you are running Exchange Server 5.0 you are able to stop the open relay function but you have to disable POP3/IMAP. This configuration can be very limiting because the only way to connect to the Exchange server is via Microsoft messaging software such as Outlook, leaving popular email programs such as Netscape and Eudora functionless when trying to connect. This version of the software should also

Jeremy Stewart (stewart003)

be upgraded to version 5.5 with at least Service Pack 2 and the encapsulated SMTP relay patch. If you are running Exchange version 5.5 upgrade to the latest Service Pack which is 3 or at least to 2 with the above mentioned hot fix. The configuration that I will be discussing will be on Exchange Server 5.5 with SP3 installed.

Internet Mail Connector

The Internet Mail Connector (IMC) is the service that is installed to allow your Exchange Server to act as an SMTP server. By default this service is not installed during installation, instead it is installed by running the Internet Mail Wizard after the exchange installation is complete. To run the Internet Mail Wizard go to File → New Other → Internet Mail Service. By default the wizard does not put any controls on who can use your Exchange server as a relay. After you have your Exchange server installed with the default settings of Internet Mail Connector service your exchange server is vulnerable to open relay.

Configuring Internet Mail Connector To Stop Open Relay

Since all the configuration changes happen in the IMS, the first step is locating the properties for the service. Open your Exchange Administrator program and connect to the Exchange server that has the IMS service installed. You will notice that the Exchange Administrator is set up just like Windows Explorer with Containers on the left hand side and objects on the right hand side. Once open find the *Connections* container located under your <organization>\<site>\configuration container in the left hand column. Once highlighted you will notice connector objects on the left hand side, one should be named *Internet Mail Service (<server name>)*. You can view the IMS properties by double clicking on it. Once open you will see several tabs, locate the *Routing* tab and click on it to view the routing properties.

The first thing you notice near the top of the properties sheet is the option of *Do not reroute incoming mail* or *Reroute incoming SMTP mail (required for POP3/IMAP4 support)*. The obvious choice would seem to be the first, but, do not use it for your system will not relay messages, but will receive them and then send a non-deliverable message back to the return address of the message. This is not good because first it put undo burden on your email system by accepting potentially very large email messages but could also be used as a reverse UCE attack with your system involved. The best selection here is the second selection.

Next you see a box titled Routing. On the right hand side of the screen select the add button. In the *'email sent to this domain'* enter your domain name. Next select the option *'should be accepted as "inbound"'* indicating that these are the only domains that the SMTP server will accept mail for.

After you have set all of the domains that your server will be accepting mail for click on the *'routing restrictions'* to open your *'routing restrictions'* properties page. The first option is *'Hosts and Clients that successfully authenticate'* which allows relaying of

Jeremy Stewart (stewart003)

messages to only users that have accounts on your server or another way to validate who the user is with the server. The next option is **'Host and Clients with these IP addresses'**. With this option you can specify by IP address who is allowed to relay through your system or what subnet is allowed to relay through your system. For example a single IP address would put in their address and the subnet mask of 255.255.255.255. For a subnet you would specify the network portion of the IP address and let 0 represent the client addresses with the subnet mask to match. The next option is **'Hosts and Clients connecting to these internal addresses'**. What this does is allows relaying of clients who can access a specific interface on a multi-homed system. Do not check this unless you have reason to do so. And the last option you have to prevent open relaying through your Exchange server is **'Specify the hosts and clients that can NEVER route mail'**. This option is pretty self-explanatory and works by denying specific IP address or subnets.

After all the changes have been made to secure your SMTP server you have to stop and restart the **Microsoft Exchange Internet Mail Service** located in the services on the control panel.

This concludes my paper on Open Relay and configuring Exchange server to not being an open relay system.

© SANS Institute 2003, Author retains full rights.

Jeremy Stewart (stewart003)

References:

Edwards, Mark Joseph. "Who's Using Your Mail Server?." 31 Aug 2000
<http://www.windowsitssecurity.com/Articles/Print.cfm?ArticleID=15480> (10 Oct 2000)

Howard, Mark. "Coping with Unsolicited Email" 1 Oct 1999
<URL:http://www.exchangeadmin.com/Articles/Print.cfm?ArticleID=6174> (10 Oct 2000)

Microsoft. "Inside Exchange Internet Mail Service" 2000
<URL:http://www.microsoft.com/exchange/techinfo/InsideIMS.htm> (10 Oct 2000)

Minasi, Mark. "Untangling Email" 1 Apr 1998
<URL:http://www.win2000mag.com/Articles/Print.cfm?ArticleID=3024> (10 Oct 2000).

Reavis, Jim. "Are you an accidental spammer?." 23 Aug 1999
<URL:http://www.nwfusion.com/newsletters/sec/0823sec1.html?nf> (10 Oct 2000)

Redmond, Tony. "Exchange 2000 and SMTP" 9 Feb 2000
<URL:http://www.win2000mag.com/Articles/Print.cfm?ArticleID=8140> (10 Oct 2000)

Toombs, Douglas. "Junk Email – Protect your Exchange Server from Junk Email." 1 Aug 2000
<URL:http://www.winntmag.com/Articles/Print.cfm?ArticleID=3673> (10 Oct 2000)

© SANS Institute 2003, Author retains full rights



Upcoming SANS Training

[Click Here for a full list of all Upcoming SANS Events by Location](#)

SANS London 2009	London, United Kingdom	Nov 28, 2009 - Dec 06, 2009	Live Event
SANS WhatWorks in Incident Detection Summit 2009	Washington, DC	Dec 09, 2009 - Dec 10, 2009	Live Event
SANS CDI East 2009	Washington, DC	Dec 11, 2009 - Dec 18, 2009	Live Event
SANS WhatWorks in Data Leakage Prevention and Encryption Summit 2010	New Orleans, LA	Jan 07, 2010 - Jan 12, 2010	Live Event
SANS Security East 2010	New Orleans, LA	Jan 10, 2010 - Jan 18, 2010	Live Event
SANS AppSec 2010 and WhatWorks in AppSec Summit	San Francisco, CA	Jan 29, 2010 - Feb 05, 2010	Live Event
SANS Phoenix 2010	Phoenix, AZ	Feb 14, 2010 - Feb 20, 2010	Live Event
SANS Tokyo 2010 Spring	Tokyo, Japan	Feb 15, 2010 - Feb 20, 2010	Live Event
SANS Geneva CISSP at HEG 2009 Autumn	OnlineSwitzerland	Nov 23, 2009 - Nov 28, 2009	Live Event
SANS OnDemand	Books & MP3s Only	Anytime	Self Paced